From: Tabish Mustufa [/O=INTUSURG/OU=MAIN/CN=RECIPIENTS/CN=TABISHM]
Sent: 5/25/2011 5:43:12 PM
To: Ted Walker [Ted.Walker@intusurg.com]; Joe Orban [joe.orban@intusurg.com]; Tyler Morrissette [Tyler.Morrissette@intusurg.com]
CC: Thomas Cooper [Tom.Cooper@intusurg.com]; Brandon Garbus; David Long; Marc Tognaccini [Marc.Tognaccini@intusurg.com]
Subject: RE: RFID Meeting Action Items

In my initial thoughts on this, there are two threats we're worried about:

1.Reprocessing: Take an expired instrument and restore its available lives
2.Counterfeiting: Take a non-ISI-designed instrument and put valid data on a tag so that it is accepted by our machine

We'd like to make both of these difficult with the security features on our tag. Reprocessing seems the more likely threat.

Actually encrypting the data on the tag doesn't buy us much, other than obfuscating trade secrets (e.g., DH parameters) encoded in the tool data. Someone trying to work around our security can copy encrypted blobs of data around without understanding what's in them.

A laser-marked unique id gives us a method to deter counterfeiting. In the Dallas implementation, we compute a cryptographic hash of the laser id and store it as part of the tool data. This makes it so that you can't copy the blog of data from one tag to another – each tag has a unique set of data on it. I think the important thing for this number is that it's a physical feature of the chip, not programmed into it, and that, as much as possible, it's guaranteed by the manufacturer to be unique. If another customer can walk up to them and ask for specific laser-marked id's, that's a vulnerability.

As an aside, we go to some lengths to hide the cryptographic hash function in an FPGA in Gemini, which suggests to me that it's a symmetric cipher. Going forward, we should use an asymmetric key "digital signature" algorithm so that we don't need to hide anything in the released software (i.e., the secret key stays on our manufacturing floor, and doesn't need to be in every robot).

The unique id doesn't prevent reprocessors from putting lives back on our instruments. In principle, you could copy the blob of data off a new instrument, then put that same blob of data back on once it's expired, and it will be as good as new. I believe the Dallas implementation uses a "write once" region in the tag to ensure that decremented lives stay decremented.

It seems to me that we want something to physically change in the tag (e.g., blowing a fuse) as we expire lives in the instrument. We do have something like that from Atmel. If we can't get it from Baylogh's tag suppliers, we would leave a pretty significant vulnerability.

-Tabish

From: Ted Walker
Sent: Wednesday, May 25, 2011 3:33 PM
To: Joe Orban; Tyler Morrissette
Cc: Tabish Mustufa; Thomas Cooper; Brandon Garbus; David Long; Marc Tognaccini
Subject: RE: RFID Meeting Action Items

Hi Joe and Tyler,

Okay, Rod and Greg want me to be the software person from Orion looking into options for security. I am not exactly an expert in this area, but I know what we do today and why. Also, I just talked to Tabish, and he, Tom Cooper, Marc Tognaccinni and David Long are looking at their options in case Atmel does not work out for them. So, it sounds like there are quite a few of us interested all in the same thing.

I realize you guys are mainly looking at cannula, and have different requirements. Maybe we should talk on the phone tomorrow.

Ted.

From: Rodney Vance
Sent: Wednesday, May 25, 2011 1:47 PM
To: Ted Walker
Cc: Gregory Toth; Boris Foelsch; Christopher Raymond; Brandon Garbus; Joe Orban; Tyler Morrissette
Subject: FW: RFID Meeting Action Items

Ted,

Can you give Tyler a little guidance?

Thanks,

Rod.

From: Joe Orban
Sent: Wednesday, May 25, 2011 12:56 PM
To: Rodney Vance
Cc: Tyler Morrissette
Subject: RE: RFID Meeting Action Items

Rod,

Although we have learned that adding a unique ID should be simple, there are details about this that we would like to run by some one.

For example, one supplier said they can do 18 digits for the unique ID. We get to define it, such as Date Code+SN# ID, or Just SN# ID, etc.

Is there a point person Tyler can contact regarding the details of our ID and or encryption details? Ted Walked seemed like he knows a lot in this space?

Let me know who we should work with.

Thanks,
Joe

From: Rodney Vance
Sent: Tuesday, May 24, 2011 10:05 PM
To: Tyler Morrissette; Aaron Carrano; Joe Orban; Marc Tognaccini; Dean Hoornaert; Brandon Garbus; Stanley Fung;

Joshua Radel; Thomas Cooper; Randy Goldberg; Greg Dachs; David Long; Gerry Labonville; Lisa Heaton; David DeTroy; Ted Walker; Katie Stoy; William Burbank; Scott Harrington
Cc: Sal Brogna
Subject: RE: RFID Meeting Action Items

Team,

I spoke with Sal and he is directing us to keep encryption as a design requirement and although he likes the idea of monitoring instrument usage via da Vinci Connect, he wants us to retain the instrument based encryption approach since we will not be able to count on Connect.

It is important to note that retaining the encryption approach does not imply that we have to stay with Atmel. We need to choose the best RFID vendor/partner based on business criteria looking forward and not allow the selection process to be unduly weighted by Ducati usage or the fact that current production encryption processes are Atmel based.

Regards,

Rod.

From: Tyler Morrissette
Sent: Tuesday, May 24, 2011 7:21 AM
To: Aaron Carrano; Joe Orban; Marc Tognaccini; Dean Hoornaert; Brandon Garbus; Stanley Fung; Joshua Radel; Thomas Cooper; Randy Goldberg; Greg Dachs; David Long; Rodney Vance; Gerry Labonville; Lisa Heaton; David DeTroy; Ted Walker; Katie Stoy; William Burbank; Scott Harrington
Subject: RFID Meeting Action Items

See meeting action items below.

Also this morning I spoke with Balogh about laser marked unique IDs and they said that this is already something they do for other customers and they would be able to provide to us. They are also looking into what memory we can fit in a small package we are looking for. There could be some technical limitations to 64 kbits of memory and as a company we might have to live with 32 kbits of memory.

- Tyler to investigate number of autoclave cycles an instrument must survive for a 10 use instrument (including autoclaves for instruments that aren't used during a case)
- Rodney to speak with Sal about the requirement for encryption on Orion Instruments and Cannulas
- Tyler to speak with tag manufacturers to see what they can offer (unique IDs, ect)
- Tyler to send sample tags to lab (Stress Engineering Services) to profile their autoclave (no pre-vacuum)
- Tyler, Joe and Brandon to have meeting with Tag companies to discuss antennas and read distances
- Tyler to investigate number of lives on Extend Training Instruments
- Mark to provide Tyler with 100 samples of the new 11x17 Atmel tag off the new reel of 10K tags